AU/ACSC/97-0603/97-03

THIRD WORLD COMPUTER SYSTEMS:

A THREAT TO THE SECURITY OF THE UNITED STATES?

A Research Paper

Presented To

The Research Department

Air Command and Staff College

In Partial Fulfillment of the Graduation Requirements of ACSC

by

Major Al G. Keeler

March 1997

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense.

Contents

Page

DISCLAIMER ii

PREFACE iv

ABSTRACT v

INTRODUCTION 1

BACKGROUND 4

THE COMPUTER REVOLUTION 7

INDIA: A NEW SOFTWARE POWER 12

IRAN: A GROWING THREAT 20

BULGARIA: HOME OF THE CYBERPUNK 28

IRAQ: POISED TO REBOUND 33

SOLUTIONS 39

CONCLUSION 45

BIBLIOGRAPHY 48

Preface

This paper deals with a topic that should be of interest to all of us who are in the business of defending this country—namely the proliferation of computer systems to third world countries. I've researched this area to prove that the proliferation and use of computer technology will have a major impact upon the security of the United States as we head into the next century.

I certainly want to acknowledge the help and support of my wife Stephanie and children A.J. and Ashley during the preparation of this work. I also want to acknowledge the always professional and courteous staff of the Air University Library for their help in researching the details of an emerging security problem for the United States that has only recently garnered attention.

Finally, I'd like to thank my research advisor, Major Mark Devirgilio, for his guidance and support in the completion of this project.

AU/ACSC/97-0603/97-03

Abstract

The United States has historically maintained a technological edge over its adversaries, used that edge to deter and, if necessary, defeat those adversaries in battle. The question to be examined in this research project is as follows. Have potential third world adversaries acquired advanced computer system capabilities that threaten the security of the United States?

The method employed is to first research trends in global computer system availability to include export policy, trade agreements, and the changing strategic environment. Next, I examine a representative group of Third World countries to assess their capabilities and examine the vulnerabilities of the US as it pursues its interests. Finally, I present proposed solutions to the threat based upon the writings of military and civilian experts in the field of information warfare.

Chapter 1

Introduction

> *the capabilities of technological mercenaries, and the capabilities of nation-states are all threats we must face. Their intentions are secondary. If a group or an individual chooses to wreak havoc, today they have the weapons to do exactly as they please.*
>
> —Winn Swartau
> *Information Warfare*

This quote by information security analyst Winn Schwartau refers to a growing menace faced by the United States—the availability of computer technology to rouge nations and groups intent upon doing harm to the United States and its national interests. During the period that some call the Computer Revolution, the United States enjoyed both a qualitative and quantitative lead in computer technology over the Former Soviet Union (FSU) and her allies. This technological advantage is reflected in US domination in military technologies such as precision guided munitions, airborne surveillance platforms, and satellite communications systems. These technologies helped the United States overcome the quantitative advantage of men and material enjoyed by the FSU and her allies. This advantage continued into the post-cold war period.

The United States demonstrated during Operations Desert Shield/Desert Storm the superiority of precision guided munitions and the force multiplying benefit of airborne and space borne surveillance platforms. Each of these capabilities are possible due to advances

in computer hardware and software technology. Iraq's 500,000 person military, equipped largely with weaponry and command and control systems bought from the FSU, was decimated by the technologically superior forces of the Coalition. This victory by the Coalition, witnessed around the world through the magic of CNN and other media outlets, was seen by many as a validation of the US strategy of technological superiority.

More importantly, Operations Desert Shield/Storm may have served as a "wake-up call" to potential third world adversaries. The major question to be addressed in this paper is as follows. Have potential third world adversaries of the United States reached a level of advancement in the computer technology arena so as to pose a threat to United States security interests?

This question will be answered by examining the following four main areas of concern:

1. Increase in availability of computer technology
2. Improvement in computer system capabilities in selected third world countries
3. Security ramifications of the proliferation in computer technology
4. Potential solutions for protection of US security interests

The increase in availability of computer technology to potential third world adversaries presents both an opportunity and vulnerability to US military leaders. The ability to disrupt the computerized command and control systems of US adversaries is a key advantage for US forces who will be at a numeric disadvantage on the battlefield of the future. The weakness in this new strategic environment is that the US reliance on computers presents a similar opportunity for adversaries possessing a low cost small computer and minimal education and training. That vulnerability is increasing as third world countries and non-state adversaries acquire more and more computer capability to

the point of potentially becoming a security threat to the US. The final point is that there are solutions both in terms of technology and in shifts in emphasis to areas such as organization, training, and education that may mitigate the new threat.

The threats to the United States are more complex in the post cold-war era. The threats are as much economic and political as they are military. Therefore, the strategy to combat the threats must be a combination of the military, economic, and political instruments of power. I also want to qualify the use of the term "adversary." Iraq's status, for example, went from a quasi ally during the 1980-88 Iran-Iraq War to an enemy in the 1991 Operation Desert Storm. Iranian military officers trained with US officers as late as the mid 1970's. Therefore, a balanced examination of third world countries, regardless of their current relationship with the US, is necessary to support the claim that the national interest of these countries coupled with the proliferation of computer technology may threaten US security interests.

Chapter 2

Background

During the Persian Gulf War, Iraq surprised many in the United States defense community by displaying an integrated air defense system that made use of French computer and communications technology. Although the United States defeated the system, the Iraqis demonstrated that sophisticated computer-based weapons are available to third world states for the right price.

Non-state actors also provide a challenge for the United States. Bulgarian computer programmers have made a name for themselves recently with a startling series of computer break-ins and their worldwide proliferation of computer viruses. These young, talented programmers present a new breed of threat to US interests. This group of people, known to some as cyberpunks, are driven, not by state interests, but by motives such as greed, ideology, and curiosity.

Another trend is the dramatically reduced cost of computer hardware combined with increased computational power and smaller footprint. Computer hardware is smaller, more powerful, and cheaper to obtain. Previous efforts at export control are no longer effective due to the expanding global economy. Additionally, the breakup of the Soviet Union has indirectly created a new competitive market for computer-based military technology that potential adversaries of the US are now pursuing. This trend combined

with the increasing reliance on commercial off-the-shelf technology (COTS) by the US military gives potential US adversaries access to virtually the same computer technology as is in use by the US military. This access also creates a vulnerability for the US as adversaries now know a great deal about US military computer hardware and software—both in terms of its strengths and weaknesses.

Third world countries are rapidly gaining the capability to optimize their military forces by using computer systems to gain situational awareness and also by using computer hardware and software as a weapon to attack the US. Several methods will be presented as ways in which these countries are posing an increased threat to US interests. These methods include traditional hacker break-ins, state-sponsored electronic terrorism, and the use of computer-based military technology such as satellite communications and cruise missile technology.

Finally, a few definitions are needed in order to understand the threat which will be examined in this research. A **computer system** is defined as a high-speed electronic device that processes, retrieves, and stores programmed information. A computer, therefore, is a system of components. The first component is the **hardware** or the physical apparatus performing the electronic operations. This includes circuit boards, keyboard, monitor and other parts necessary in computer operation. The second component is the **software** or the internally stored data, programs, or routines necessary to perform computer operations. The final component of the computer system is the **communicating device** which may be a modem, network card, or any device which allows a stand-alone computer to communicate with another device.

The use of these computer technologies by Third World countries have had a dramatic effect upon the strategic environment facing the United States. Understanding the complexities of this new environment must begin with an examination of the new computer revolution.

Chapter 3

The Computer Revolution

The 1990's have seen another type of computer revolution. A revolution, not just in capabilities, complexity, or size of computers, but in terms of worldwide proliferation and use. This proliferation of computer hardware and software has been largely driven by political, economic, and military factors.

First, the breakup of the Soviet Union and the end of the cold war created the opportunity for previously "closed" economies to open and develop free market economies. These economies have attracted interest from multi-national computer firms, in particular, who see the potential for great profit making as these countries seek to modernize their industrial and military sectors with automated tools.

The second factor in this explosion has been the emergence of a global economy and the retreat from state-controlled businesses in many sectors of this economy. One of the most dominant and growing sectors of the world economy has been computer hardware, software, and services.

The global software market alone is valued at over $77 billion with US companies accounting for 75% of that figure[1]. This market includes the sale and maintenance of operating systems, applications, database management systems, and specialized tools. In information services, or the sale of technical assistance in the design and maintenance of

information systems, industry observers predict a gain of 13 percent for US companies in 1997 adding to an already robust 46% of the worldwide market.

The US also has dominated the computer equipment sales category with over 75% of the market. US exports of computer hardware and software are expected to continue to grow due to a dramatic opening of the world economy by trade agreements such as the North American Free Trade Agreement (NAFTA) and the General Agreement on Tariffs and Trade (GATT). These trade agreements, according to experts such as Secretary of Commerce Mickey Cantor, are dramatically reducing tariffs in major US export markets. GATT signatories number 112 nations, all committed to free market economies.

The economic benefits to computer firms are staggering. According to Commerce Department figures, at least 50% of US computer industry sales are to foreign countries. Tariffs and other protection measures have held down profit potential. However, GATT induced tariff reduction in the computer export market that is expected to approach 70% . In Europe, a $10 billion market for US computer firms in 1993, tariffs will fall by 80% [2].

Clearly the world is moving toward an open and free world economy and the computer industry is one of the biggest beneficiaries of this new trade environment.

Historically, another impediment to the free flow of computer hardware to overseas markets has been restrictions by the US and NATO allies due to concerns that the computers would be used to design nuclear weapons and used in other military applications such as in air defense systems. The mechanism that prevented the spread of computer technology to the former Soviet Union and its client states such as North Korea was the Coordinating Committee on Multilateral Export Controls or COCOM. The COCOM agreement was designed to keep militarily sensitive technology out of the hands

of NATO's enemies. COCOM's membership numbered 17 nations and included all of NATO except Iceland with Japan and Australia added as signatories. The agreement was allowed to expire in 1994 after extensive lobbying by the computer industry among others, that the agreement was a product of the cold war that had outlived its usefulness. US firms, in particular, made an impassioned argument that its hands were tied due to tight regulation by US regulators while Japanese and European companies were allowed to export technology due to their country's interpretation of the rules.

The US has bowed to computer industry wishes and eased its interpretation somewhat as evidenced by recent sales of supercomputers to Russia and China, an unthinkable occurrence during the Cold War. The Cray Research Corporation sent two supercomputers, an 8-processor YMP and an entry level EL to Russia[3]. The deal with Russia's Rosgidromet agency includes two supercomputers, third-party equipment and software, and the construction of a dedicated computer room to house the systems. The sale, approved by Vice President Gore, is intended to help the Russians with their environmental and earth sciences programs.

The significance of the deal to US military security analysts is that the proliferation of complex computer technology is a certainty in the global economy even to "former" military rivals such as China and Russia. A secondary, albeit more troubling question is can Russian computing capability acquired from the US be used to benefit third world adversaries of the US? Is it possible that Iran, cash rich but computer technology poor, could enter into a "relationship" with Russia, technology rich but cash poor, in order to circumvent US-led restrictions on the sale of sophisticated computer technology?

The Russian military industry is in a very difficult position, as drastic cuts in military spending have had a devastating impact of military preparedness. In fact, the Russian army, navy, and the air force must be cut to a fifth or tenth of their previous sizes. The forces that remain are marred by low pay and deteriorating equipment in need of maintenance. Russia's civilian scientists face a similar dilemma. Sergei Kapitza of Moscow's Academy of Sciences states that "problems exist regarding the low salaries that scientists and engineers receive and the meager government support of science." Kapitza bristles at the notion that Russian scientists and engineers would sell technology to "rouge" states but he does acknowledge that technology transfer has taken place with businesses from Russia, the US, and Europe as the chief culprits[4].

The obvious conclusion is that the conditions for computer technology proliferation are at an all time high and continuing to increase. The chief suppliers have drastically reduced trade barriers through trade agreements favoring an open market. Previously "closed" economies in China, Russia, and the Middle East are openly moving toward global, free market economies which are fueled by advances in computer technology. And finally, the fall of the Soviet Empire has removed the incentive to restrict that computer and information technology hence the Clinton Administration's moves to promote the export of that technology with the end of COCOM.

The evidence clearly points to a world environment in which computer hardware and software technology can be acquired by a wider group of third world nations and actors. How has this new economic environment affected third world nations and how does that relate to the security of the United States? An examination of computer technology

trends in third world nations is key to answering these questions. One nation making great strides in the use of computer software technology is India.

Notes

[1]M. Perryman, "US Industry Remains Dominant Player in Global Markets," *San Antonio Business Journal,* 21 June 1996, 59.

[2]David S. Cloud, "Critics Fear GATT May Declare Open Season on US Laws," Congressional Quarterly,23 July 1994, 2005.

[3]*Electronic News,* 16 Jan 1995, 24.

[4]Sergei Kapitza, *The Bulletin of the Atomic Scientists,* May 1992, 8.

Chapter 4

India: A New Software Power

American fighter aircraft streaked toward the "shooter," an enemy mobile missile site just across the border. The lead pilot descended over the coordinates listed on his real-time display but saw nothing. Frustrated, he returned to base unaware that his mission had been sabotaged by a rouge programmer weeks earlier.

The US military has committed itself to the use of computer and communications technology in the attainment of full spectrum dominance[1]. Full spectrum dominance can be described as the use of computer and other information technologies to produce a truly interactive picture and a decisive military advantage. The fictional example cited above highlights the strengths and vulnerabilities inherent in that objective. The goal is situational awareness, the ability to see everything within a given area and to use that knowledge to apply the appropriate force, if necessary, to mitigate that threat. In the example, stand-off sensors detected a threat, determined its coordinates, and that information was then relayed to fighter aircraft capable of dealing with that threat.

The advantages of this "sensor to shooter" technology are obvious. A missile launch, for example, can be instantly detected, appropriate information electronically relayed to an operations center, with similar information relayed to the appropriate response team, in this example, fighter aircraft. The timeline between enemy action and friendly response is shortened with the response focused and, consequently, more lethal. The weakness of this

technology is not so readily apparent. Computer hardware and software are required to implement the technology due to the large information requirements necessary to digitally map a battlespace and relay the appropriate information to the right place at the right time. This creates a target of opportunity for US adversaries. The US is now dependent upon the computer software that is necessary to process and distribute that information. The question to be answered is do third world adversaries possess the ability to successfully attack this weakness? To answer that question requires an examination of a growing trend in the software industry, namely, the movement of the design and maintenance of software to companies and individuals in third world countries such as India.

For the past thirty years, India has been motivated to try to develop self-sufficiency in computers and electronics largely by national security concerns related to border conflicts with China and Pakistan[2]. This ambition is understandable given India's strategic environment. The country shares borders with both Pakistan and China neither of whom would be characterized as an ally. Conflict with Pakistan is well documented. Pakistan has also been steadily upgrading their military capabilities seeking help from America, Russia, and China. China, in particular, has raised the stakes in the region by selling nuclear technology to Pakistan[3] despite international pressures to support nuclear non-proliferation. India has nuclear capability having detonated a nuclear device in the 1980s. The region is rampant with military, and political conflict and competition.. This competitive strategic environment caused India to pursue strategies aimed at leveraging its technological capabilities to improve its military and economic security.

The Indian government saw that implementing policies that took advantage of its abundance of computer software professionals would directly benefit the economic growth of the Indian economy. Tariffs which limited foreign competition and imports of computer software tools were eased which. This change attracted multinational corporations (MNCs) in need of India's abundance of computer programming professionals. These computer programmers had emerged as a highly-sought commodity due to their skill and low cost in comparison to US and European programming talent. Policies such as tax incentives and the creation of software parks have aided in the remarkable growth in the number and quality of India's computer professionals. A 1992 World Bank study of eight nations rated India as the most attractive nation for US, Japanese, and European companies seeking offshore software-development partners. India has also aggressively been modernizing their data communications infrastructure. India's computer firms boast a state-of-the-art satellite communications capability allowing them to deliver software services from Indian soil and stemming the immigration tide of their talented software professionals who regularly stayed in the United States after completing software projects for American companies.

Another key to India's technological success was their efforts to grow their small computer industry while resisting IBM's large computer influence of the 1970's . India skipped the mainframe computer era positioning itself to take advantage of the smaller computer systems with their highly sought-after "client-server" technology. European and Western businesses now regularly tap India's software engineering expertise to migrate away from mainframes and to the more flexible user-friendly client-server systems which

are the state-of-the-art today. India's mastery of the English language also has made them the software guru of choice in today's highly competitive computer industry.

India's other forte is software toolkits used to build "user-friendly" graphical user interfaces (GUI). Softek, an Indian software developer, offers a software toolkit that not only supports the building of GUI but can also connect to relational database management systems (RDBMS) from industry leaders Ingres, Oracle, and Sybase, an impressive capability. Thus, Indian companies are positioned to offer customers an impressive array of computing capability which include a friendly GUI to a network of software services regardless of small, mini, and supercomputing services.

Another strategy employed by India to grow its software expertise was to create several technology parks. Companies locating at these parks enjoy common computing and telecommunications facilities including leased-line access to satellite links. They can also import equipment needed for software development duty free. N. Vittal, Secretary of the Department of Engineering states simply that, "We want to create many Hong Kong's and Singapore's." Vittal is credited with slashing government red tape, approving one joint venture license application in only four days.

Another growing trend in India is joint ventures with US. computer companies. Indian companies now supply several state-of-the-art products for US firms such as UNIX operating systems, motherboards for high-end workstations, and the manufacture of complete workstations for export. India's software exports were estimated at $1 billion in 1996 easily making them the top developing country in terms of computer technology.[4] The National Association of Software and Service Companies estimates that sales will hit $5 billion by the end of the decade.[5] Today, India's software houses have satellite links to

American banks, telephone companies, fuel suppliers, government agencies, hotel chains, and a host of manufacturers[6]. Citibank, American Express, GE, IBM, Reebok, Texas Instruments, Hewlett-Packard, and Compaq Computer are just a few of the US firms relying on Indian programmers for critical software applications. ATM machines, gas purchases by credit card, hotel reservation systems, US government agencies software maintenance contracts, etc. are a few of the many applications written and maintained by Indian programmers from their many technology parks.

Indian firms are also increasingly being tasked with the important task of writing operating system software, the sophisticated programs that tell the computers what to do. American white collar workers with salaries of $40–$50,000 per year are now competing with immigrating Indian programmers making less than $10,000 per year. Economically, this disparity has hurt workers in America with Congress responding with legislation limiting the number of visas going to foreign workers. However, the Indians and profit-hungry American corporations have thwarted that strategy by the use of satellite communications technology linking the programmers in areas such as software-rich Bangalore, India to their client information systems in the United States.

What are the security ramifications for the US? The economic impact has been examined but what about the military impact? India can hardly be characterized as a rogue state or even one unfriendly to the US but US national security analysts should take note of the fragile strategic environment in the region which drives the competition for technological superiority. Pakistan's desire to buy nuclear capability coupled with India's existing nuclear capability can be perceived as part of that competition. India's achievement in computer capability coupled with a recent infestation of Indian computers

by a virus of Pakistani origin[7] also demonstrates the new level of technological competition in the region.. India's national computer network managers reportedly immediately strengthened their security systems. This competition for technological superiority will certainly extend to an effort to obtain American technology particularly in the area of computer-based military technology. India has the computer expertise to know which systems to target and how to apply those systems for its use. Further motive for Indian action against American interests is the anticipation of a "tilt" of US support to Pakistan should a future India-Pakistan armed conflict occur. The US has a history of arms sales to Pakistan to include a proposed billion dollar sale of F-16 fighters which contributes to this speculation. This factor coupled with India's fragile strategic environment gives India the incentive to use their software expertise to plan a clandestine software attack against US military assets to prevent their use in providing valuable information to Pakistani forces during a future conflict.

Is the US vulnerable to such an attack? The fact that the US is committed to the use of commercial off-the-shelf computer equipment and software in its acquisition of military systems and the fact that Indian programmers are employed in the maintenance of this computer software creates a vulnerability that can be exploited by Indian intelligence officers. An example is the use of programmers to introduce software bugs that temporarily degrade the performance of US computer-based command and control (C2) systems without leaving "fingerprints" that could be traced back to the perpetrator. This feature could be introduced during either the design or maintenance phases of an American C2 system and be designed to remain dormant until activated by the programmer at a designated time. This tactic, used in conjunction with military

operations, would provide India with a better chance of achieving operational surprise and, consequently, the attainment of its objectives.

Another US vulnerability is that some sensitive US military communications networks are known to use UNIX-based client-server computer architecture of which Indian programmers are now the acknowledged experts, having written a significant portion of the native operating software. This provides India with a rare technological advantage that can be exploited in ways similar to the example listed above. A knowledgeable programmer can attack the critical link between the "host" computers or servers and the "end user" computers or clients. This link can either be completely shut down or simply monitored to provide valuable information for an intelligence operation.

Another method of attack as detailed by futurists Alvin and Heidi Toffler involves the "planting" of sophisticated instructions embedded in chips which are the central component of much of the world's military technology[8]. The Tofflers predict that weapon systems which depend upon information from global positioning system (GPS) satellites could be programmed to misinterpret data if in use at a given location. The system could also be programmed to accept an instruction that renders it useless to the enemy military. Both examples show that an adversary need not destroy the weapon mass on mass but rather introduce a vulnerability that can be exploited at a time or place of their choosing. A growing software power such as India is rapidly developing the capability and the access to the commercial software market to perform the "software attacks" listed above.

As mentioned earlier, India can hardly be characterized as an adversary, however, the recent (February 1997) expulsion of a US diplomat, who was reported to be the CIA

Station Chief by major news agencies, for spying by India and the US retaliation of expulsion of two Indian diplomats points out that the two countries have recognized the importance of gaining information on the other's capabilities and intentions. India is among the most proficient third world countries in terms of computer software capability, but others have the cash and motive to improve upon both their military-based computer expertise as well. One such country is Iran.

Notes

[1]Chairman of the Joint Chiefs of Staff, *Information Warfare: A Strategy for Peace...The Decisive Edge in War,* (Washington D.C.: Government Printing Office), September 1996.

[2]Jason Dedrick and Kenneth Kraemer, *Asian Survey,* May 1993, 490.

[3]*The Oil Daily,* "US Decides Against Sanctions Over Sales of Nuclear Technology to Pakistan," 13 May 13 1996, 9.

[4]Byte Magazine, September 1993

[5]John Stremlau, *Foreign Policy,* "Dateline Bangalore: Third World Technopolis, Spring 1996, 152.

[6]*Foreign Policy,*152.

[7]K.S. Jayaraman, *Nature,* "Pakistani Virus Invades Indian Neighbor,"13 April 1989, 530

[8]Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*(Boston, MA: Little, Brown, and Company, 1993),233-234.

Chapter 5

Iran: A Growing Threat

A group of federal agents swarm a freight warehouse at the Port of Long Beach, Calif. and seize two crates. Did they seize missiles? Aircraft parts? Top Secret military plans bound for Russia? No, the crates contained a $1.4 million satellite-communications system driven by a high-end Sun Microsystems computer intercepted before shipment to Iran.

This true story highlights an ongoing war between Iran and the US, the battle to control sophisticated military technology[1]. In 1993 alone, according to Frank Deliberti, director of export enforcement at the Commerce Dept., the US investigated over 165 companies for shipping sensitive technology to Iran, a 700% increase from five years ago[2]. Military equipment seizures are nothing new, the US battled the Former Soviet Union (FSU) on that front for years. The difference in this case is the drive against a third world country and that the emphasis is not just on traditional military gear, but on "dual-use" technologies, in particular, computer hardware and computer-based technology. Why the emphasis? One reason is the improving technical prowess of third world countries such as Iran.

Since the August 1988 cease-fire in its war with Iraq, Iran has quietly adopted a free-market economy and is attempting to match the economic and military progress of both its neighbors and the rest of the world. The result of this competition is that Iranian military, government, and private business interests became extremely hungry for computerization.

Economic, social, and political upheaval combined with US computer export restrictions had caused Iran to lag behind in the computer revolution but steps are being taken to remedy the situation. First, Iran has been able to circumvent a US-led economic boycott by buying equipment from friendly nations such as Turkey and North Korea[3]. They've also been able to circumvent US restrictions on computer exports by buying computers from East Asian companies like Tatung and also through European companies.

Another strategy has been to buy computer components abroad and use them to make quality clone computers. These small computers, running Microsoft's MS-DOS operating system, are quality IBM-clones capable of running most industry-standard applications to include access to the Internet. Unlike India, Iran has had to overcome a language barrier as the average Iranian user needs the Persian character set vice the standard English character set, but the Iranians seem to be able to work around the difference and have sustained a steady growth in their computer market, according to Saeed Vahid, a technical writer based in Tehran[4]

The trend most troubling to US security analysts has been Iran's extremely aggressive pursuit of US state-of-the-art computer technology despite the ban. One such instance was the case of the illegal attempt at exporting an IBM ES 9000 mainframe computer to Iran in January of 1993. Despite the fact that the Commerce Department denied an export license, two Orange County men operating businesses under the names Lucach Corp., Computer World, and Iran Business Machines tried to ship the $1.4 million computer to Iran via France[5]. An elaborate scheme was devised in which the computer was bought from IBM by one company under the pretense that the machine was for domestic use. The computer was then to be shipped to France, and a sister company,

prior to its routing to Iran. The Iranian Ministry of Agriculture would make the $2 million payoff to Computer World through the French Company to disguise the transaction. The computer was intercepted and the two men indicted before the transfer took place, however, but this incident highlights the Iranians desire to acquire the computer technology it needs to compete economically and militarily in today's strategic environment.

A factor working in Iran's favor is that US companies are not completely sold on US embargo efforts, having lost major business deals due to export restrictions. BP America recently opted not to apply for a potential $100 million contract for chemical manufacturing equipment to Iran while Boeing and GE were denied a potential $750 million contract for Boeing 737s with GE engines. Europe's Airbus was ready and willing to fill the void.

US military leaders are also increasingly concerned with Iran's apparent intention to become the number one military and economic power in the Middle East and destabilize the region by spreading Islamic Fundamentalism and anti-Western politics. Martin Indyk, the National Security Council's (NSC) senior director for Near East and South Asian affairs, warned that Iran could exceed Iraq's pre-1990 military power by 1998 if preventive steps are not taken. "Through its active efforts to acquire offensive weapons, Iran is seeking an ability to dominate the gulf by military means"[6].

Iran has also reportedly conducted a massive military buildup on Abu Musa, a small island at the mouth of the Persian Gulf from which it can use its increased military might to threaten Gulf oil shipments.[7] Iranian armaments on the island include HAWK and SA-6

air defense missiles and "Silkworm" surface to air missiles which are capable of striking ships.

The NSC has also steadfastly maintained Iran on its list of states known to support terrorism. State-sponsored terrorism was also the main reason given for President Bill Clinton's decision to gain a total economic embargo against Iran in 1995. Some US business executives opposed the ban stating that it would only aid competitors from other countries but the Clinton Administration has maintained the ban, in fact strengthening the embargo by seeking to punish nations who trade with Iran[8].

Iran, however, has not been deterred in its efforts to get computer and military technology. While publicly stating that its only goal is to replace defenses decimated during its war with Iraq, Iran has actually bought a significantly improved capability. In addition to computer and satellite technology, Iran has purchased advanced weaponry such as cruise missile technology from North Korea, submarines from Russia, and jet fighters from China. The missiles, intended to sink aircraft carriers, are deployed along the tanker routes in the Strait of Hormuz, according to US. military and intelligence analysts[9]. Iran also has active nuclear and chemical arms programs according to Yossef Bodansky, director of the Republican Task Force on Terrorism & Unconventional Warfare despite continued denials by Iran.

The motives for this Iranian buildup of computer-based military technology lie in the recent history of the Middle-East. First, the current Iranian government was created during the deposing of the US-backed regime of the Shah of Iran during the 1970's. The Iranian revolution resulted in the overthrow of the Shah, the taking of American hostages, and a suspension of diplomatic relations that continues today. For the current Iranian

leadership, America has been characterized as the "Great Satan" which will eventually be destroyed in a holy war. The Iran-Iraq War of 1980-88, which produced over 600,000 casualties, is also deeply ingrained in the hearts and minds of the Iranian leadership. The US backed Iraq during the war which exacerbated tensions between the leadership of the two countries as had the storming of the American embassy by Iranian revolutionaries in 1978.

Another strain between the US and Iran is the belief by some leaders in the US that Iran sponsored the terror bombing of a US military housing complex in Saudi Arabia killing 19 US servicemen[10]. That assertion was rejected by Iran with the Iranian foreign minister threatening retaliation for any US attack against Iran. Additionally, Iran's desire to improve its computer-based military technology is based upon the quick and decisive victory by the US-led coalition in Operation Desert Storm. American weapons were showcased during the war, particularly the computer-based technology that allowed the US to obtain a situational awareness that was critical to decimating the Iraqi armed forces. The Iranians saw, through the media, that the US could see the Iraqi positions, maneuver coalition forces into an advantageous position, and destroy the Iraqi forces at a lightening pace. The Americans could see the battlefield and control their forces and the Iraqis could not. Iranian military leaders know that any future conflict will be won or lost based upon acquiring the computer technology that is crucial in winning the competition for information superiority

The offensive methods used by Iran in future conflict will be radically different from those seen in Operation Desert Storm. A recent assessment by Pentagon security analyst Andrew Krepinevich calls the new Iranian approach "street fighter" tactics. In addition to

sponsoring terrorist attacks against US interests, the Iranians will continue to build up their traditional army capabilities. These include armor, infantry, and special forces along with a new effort in obtaining new missile technology to disrupt any American deployment to the gulf. Iran would attempt to overwhelm enemy airfields, command and control centers, and aircraft carriers in the region with its new missiles to neutralize the US air, land, and sea buildup. Another major difference will be seen in their use of computer-based technology to prevent the US from obtaining the overwhelming information dominance seen in the Gulf War. The use of computerized satellite communications systems to maintain command and control of their forces is another tactic Iran will employ to maintain the control over their forces that the Iraqis lost during Desert Storm.

Another tactic in Iran's arsenal is the ability to "rent" an individual or group of information warriors with the goal of attacking American military and civilian computers. Mark Thompson of Time Magazine recently detailed a ten day information war by Iran set in the year 2000 that virtually paralyzed America by attacking military, government, and civilian computers with logic bombs, viruses, and electronic break-ins. This infowar was a RAND Corp. war game played by senior US officials[11] which highlighted the destruction that was possible by an organized, well-financed group of cyberterrorists.

Is America really vulnerable to such an attack? The Pentagon's Defense Science Board warned of such an attack in 1994 with its assertion that the computers running the nation's power plants, airports, banks and telephones are ripe for ruin.[12] Although Iran does not yet have the native computer capabilities to pull off such an attack, the needed capabilities may be available "off the shelf." According to some Pentagon officials,

hackers may be the new mercenaries[13] and a motivated, oil rich state, such as Iran could easily find individuals or a group of hackers and sponsor their efforts to electronically destabilize American interests.

This extremely active buildup of military technology and apparent link to terrorist groups is of great concern to the Clinton Administration which has led efforts to economically isolate Iran. This resolve is obviously a product of the painful lesson of Operation Desert Storm in which American servicemen were attacked by Iraqi weaponry purchased from American companies. As US military analysts keep a wary eye on the technology buildup in Iran, America's civilian leadership wants to avoid a repeat of 1991 in which America had to destroy an enemy it helped to arm. European firms have not heeded the US call for an economic boycott of Iran and have helped to rebuild Iran's infrastructure and military capability in exchange for oil and oil profits.

As stated above, another new threat is the ability of a third world adversary of the United States to "rent" cyber warriors for the purpose of launching computer attacks. One potential source can be found in the Former Soviet Union.

Notes

[1]Michael Schroeder and Larry Armstrong, "The Push to Plug Iran's Technology Pipeline," *Business Week,* 14 June 1993,31.

[2]*Business Week,* 31.

[3]*Time Magazine,* "The Pyongyang-Jerusalem Connection," 31 May 1993,16.

[4]Saeed Vahid, *Byte Magazine,*"Moving Forward Cautiously," October 1993,48.

[5]Michelle Vranizan, *The Journal of Commerce,* "Two Charged With Trying to Ship Computer to Iran,"26 Jan 1993,10A.

[6]*Business Week,*32.

[7]Arthur Gottschalk, *The Journal of Commerce*, "US and Iran Headed for a Showdown?," 12 August 1996,7B.

[8]Jonathan Bearman, *The Oil Daily,13* August 1996.

[9]*Business Week,*33.

[10]*The Journal of Commerce,7B*

Notes

[11]Mark Thompson, *Time,* "If War Comes Home," 45.
[12]*Time,*45.
[13]*Time,44.*

Chapter 6

Bulgaria: Home of the Cyberpunk

During the Gulf War, according to Pentagon officials, a group of Dutch hackers offered to disrupt the US military's deployment to the Middle East for $1 million[1]. Saddam Hussein spurned the offer, but, according to a Pentagon advisory panel, the potential for disruption was great.

Another factor in the third world computer revolution is the new wave of talented programmers in the former Soviet Union. Bulgaria offers a revealing look at the future of FSU technical talent as they offer a tremendous group of computer programmers, hundreds of whom have been hired by Western companies in recent years. As in India, these bright young programmers write software for salaries of $10,000 to $20,000 or about one-fifth of what US-based programmers earn[2].

Western companies have been quick to take advantage of this cheaper, albeit technically proficient workforce. Critics, however, see the shift of programming work as a threat to US long term economic security as proficiency in the computer software business shifts to foreign countries, some of whom may not share America's interests. "As critical talent locates abroad, critical innovation might too," says Robert Forman, an industry executive based in New York City[3] One US multimedia firm, Great Bear Technology, exported 85 programming jobs to Bulgaria using minimal US programmers whose only task is to assemble the code developed by the Bulgarians. Executives at Great Bear insist that Bulgaria is loaded with computer talent due, ironically, to the restrictions

placed on the country during the cold war. Several of the Bulgarian programmers learned programming on older IBM 360 and PDP-11 minicomputers smuggled to the East Block during the height of the cold war in violation of Western export controls. The programmers did not have the benefit of US training or programming aids and thus learned their skills by programming at more of a "systems" or technical level.

Today, with the benefit of programming aids and documentation, these programmers and their protégés churn out sophisticated design quickly and efficiently making them a hot commodity with Western businesses. Sun Microsystems has been so impressed with the FSU talent that they have turned over critical tasks such as operating system design and network security software improvements to these programmers[4].

The picture from Bulgaria is not 100% good news for US businesses, however. A new breed of programmer has developed in Bulgaria. Native Bulgarian and University of Hamburg computer expert Besselin Bontchev calls these individuals "technopunks"[5] These individuals are to computers and networks what terrorists are to the rest of society. They inflict destruction on unsuspecting networks by infecting the computer with viruses or software designed to change or alter data or programs. Bontchev identifies Bulgaria as the leading producer of technopunks or cyberpunks as they're called by many in America due to several factors:

1. Unemployment or underemployment of young people
2. Widespread software piracy
3. Lack of legal remedies to restrict their actions
4. Social conditions creating a group of young, under socialized individuals

These young people regularly communicate and terrorize the Internet using such nicknames or "handles" as Dark Avenger, Phiber Optic, and The Leftist or in groups with

names such as The Legion of Doom, and Masters of Deception. Therefore, Bulgaria offers an interesting contradiction: a sought after workforce of programmers and a ruthless group of young people intent on destruction of some of the same computer networks.

Again, central to the argument of this paper is that Western businesses are increasingly becoming reliant upon programmers from foreign countries that may attack from the most vulnerable place in any organization, from within the organization. Developers of operating system software and security software routinely have the knowledge and access to attack directly or indirectly systems they are responsible for. Placing that kind of power in the hands of foreign workers is a risk to US security.

In terms of US national security, the biggest risk is that third world countries are now making tremendous strides in the development of the very software systems the US government buys and operates as part of its mission critical computer systems. The fact that this software is developed and maintained by FSU programmers, to include Bulgarians, must be taken into consideration. As more and more development work flows to third world countries, will the maintenance call from a military operator running a mission critical computer system in Germany be routed to Bulgaria for software support? What kind of individual is at the other end of that phone? A hard working professional or a cyberpunk?

As the American military shifts to smaller computers with more robust networks, the risk of virus infection grows according to Mr. Bontchev. Larger computer systems such as mainframes had a more inherent security environment while the new smaller computers are more likely to be networked and more likely not to have a mature security

environment. An estimated four thousand different types of viruses are currently in circulation in the US with practically all of these written for small computers. The majority of these viruses are harmless and easily cleaned but the biggest effect of the attack is not the virus itself, but the resultant lack of confidence in the data and in the system the virus leaves behind. The Dark Avenger need not destroy a military network to accomplish his objective but rather simply randomly change data so as to cause the entire information base to be suspect. A joint task force that cannot trust its data could be forced to not use that system rather than risk acting on inaccurate information.

This vulnerability threatens the goal of information dominance for US warfighters and significantly levels the technological playing field. As futurist, Alvin Toffler stated recently, "It's the great equalizer. You don't have to have to be big and rich to apply the kind of judo you need in information warfare. That's why poor countries are going to go for this faster than technologically advanced countries.[6]"

Another vulnerability is DOD's increasing reliance on commercial off the shelf (COTS) hardware and software. The use of COTS in military systems makes those systems familiar to sophisticated adversaries and also exposes those systems to software developers and maintainers who are not subject to US security regulations[7]. Therefore, the threat to US national security as presented by Bulgaria is not as a result of state action, but by Bulgarian individuals and groups instead. As stated above, cyberpunks can either act alone or in groups. They also offer an attractive target for a cash rich, computer technology poor third world state looking to "buy" an information warfare capability for use against an adversary. Iran is one state linked in the past to "sponsoring" terrorist groups against US interests and, in this case, could sponsor a group of Bulgarian

cyberpunks to attack US civilian computer targets. Another state that has challenged the US using computers and computer-based weaponry is Iraq.

Notes

[1]Douglas Waller, *Time,* "Onward Cyber Soldiers,"44.

[2]G. Zachary, *The Wall Street Journal,*"U.S. Software: Now It May Be Made in Bulgaria," 21 February 1995,1.

[3]*The Wall Street Journal,*1.

[4]*The Wall Street Journal,*1.

[5]*Data Communications,*"From Russia with Bugs," Feb. 1996,19.

[6]Douglas Waller, *Time Magazine,* "Onward Cyber Soldiers," 21 August 1996, 43.

[7]David S. Alberts, *The Unintended Consequences of Information Age Technologies,*,(Washington D.C., Library of Congress), October 1996.

Chapter 7

Iraq: Poised to Rebound

> *Jan 199.....Task Force Normandy, a force of Air Force Pave Low helicopters escorting Army Apache helicopters lifted off from Al Jouf in western Saudi Arabia. Their objective—a night raid on two clusters of Soviet-made early warning radar just north of the Saudi-Iraqi border. The radar were operated from mobile vans and were the "eyes" of a surprisingly complex Iraqi computerized air defense system known as Kari. Over a four-minute period, the teams fired over thirty Hellfire missiles and dozens of 70mm rockets destroying generators, antennas, personnel, and command vans ensuring that the ensuing successful air attack of the Kari nodes would have the element of surprise...*
>
> —Michael Gordon and Bernard Trainor
> *The General's War: The Inside Story of the Conflict in the Gulf*

This attack illustrates the importance that Desert Storm planners placed in the destruction of enemy command and control, an emphasis that certainly is not new to US military planners. What was new in this case, however, was the technical sophistication of the system they set out to destroy.

Iraq had constructed, using Chinese, Soviet and Western technology, a computer-based air defense system unlike any in the third world. This system, similar in some respects to one deployed by the British in W.W.II, used "spotters" or personnel deployed along the border to spot enemy aircraft. These spotters could feed information using hand-held devices into regional Intercept Operations Centers (IOC). These IOCs were mobile communications vans parked inside concrete bunkers and were manned by air defense

officers. These officers, equipped with radarscopes could direct Iraqi fighters and pass targeting information to anti-aircraft batteries and SAM sites. The system was built with ease-of-use in mind as all the officer had to do was to touch a light pen to a screen in order to track aircraft. The IOCs were tied in a pyramidal structure to higher level Sector Operations Centers, three story command centers built of reinforced concrete, and manned by officers with responsibility for directing the air war in larger sectors of Iraq[1].

At the heart of the system, and a high priority for Desert Storm planners was Kari, the mainframe computer complex built by the French aerospace firm, Thomson-CSF, housed at Air Defense Headquarters in Baghdad. Kari also was linked to a computerized battle management system called ASMA, developed by the British, that was used to manage logistics distribution. The spotters, IOCs, and SOCs were tied together by redundant communications to include microwave shots, buried fiber optic cable and copper lines, field radios, and telephones. The redundancy of the communications made early warning a concern for coalition planners. Thomson designers built a system simple enough to be operated by controllers with a sixth-grade education. The mainframe computer at the heart of the complex was 70's technology but achieved its purpose of managing the type of air war that a third world dictator would expect.

The Kari system served three primary purposes for Saddam; 1) early warning of air attack , 2) provide targeting information for Iraqi gunners and intercept aircraft; and 3) provide a "picture" of the battlefield, a must for Saddam who insisted on centralized control. When combined with the arsenal bought over a number of years by Saddam to include SAMs and shoulder-fired missiles and early warning radar some of which were of the difficult to jam variety, the air defense system certainly provided a dangerous

environment for attacking aircraft. Central to the claim in this paper is that the use by Iraq of a computer system and its capabilities and limitations provide valuable insight as to the military technology goals of third world nations.

How did Saddam obtain western computer technology specifically built for military purposes? The answer is simple. Iraq was cash rich and technology poor and simply contracted with a French firm that was technology rich and cash hungry. Thompson violated no laws in the 1980's when they designed the Kari system. However, their behavior as the war approached bears study. American intelligence officials reportedly had great difficulty extracting capabilities and limitations information from Thomson who decided to protect the privacy of their client and/or future profits from the sale or upgrade of similar systems to other third world countries[2]. Apparently, the destruction of Kari would have a negative impact on the profit margin for this multinational corporation.. It took intervention by the Bush Administration through the French government to learn Kari's secrets.

The French designers did pass on valuable information, that the software was limited to only tracking 120 aircraft per command center under optimal conditions. This was a significant capability for a third world conflict but not sufficient to thwart a coalition attack. Also, due to the hierarchical nature of the systems implementation, taking out the right sites would "blind" a select Iraqi sector, opening a vector for attackers to blow through on their way to Baghdad and the heart of the system. And, as is the case with hierarchical systems, once the brain is dead, the body or Kari system is dead. Armed with this knowledge, the coalition planners built a devastating campaign plan and destroyed the

Kari system. The Iraqis lost the air defense battle, in essence, as soon as its secrets were learned.

American lessons learned have been discussed in many works since 1991 but what were the lessons learned for the third world and in this case the Iraqis? One lesson has to be that they were on the right track with their attempt to use a combination of no technology (spotters) and high technology (computers and communications) in order to gain and maintain situational awareness. A second lesson is that fixed, hierarchical implementations of that technology are simply "soft" targets to their enemies. The new systems have to be mobile, flexible, and redundant with computers that are smaller, faster, and easier to set up and operate. Communications methods must have similar flexibility and mobility. Satellite communications is the obvious application here. A mobile satellite communications terminal driven by a small computer workstation would be a prime addition to a rebuilt Iraqi command and control system and, as was shown by the earlier discussion on Iran, this technology is available for a reasonable price. Fixed communications sites will also migrate to smaller, redundant satellite terminals as well which would make these sites more difficult to target for US military operators.

Is there any evidence of this modernization occurring? Certainly, the current (Jan 1997) Clinton Administration-led economic embargo has stopped Iraqi arms purchases but the embargo may not last much longer. Western countries such as France have wanted to resume trading with Iraq for some time and the Russians, cash poor and owed $12 billion by Iraq, also have a huge stake in allowing Iraq to sell oil and buy "defensive" weapons[3]. Programming and engineering talent is abundantly available from Russia, Bulgaria, India, and France. Those countries alone could outfit Iraq with a newer, more flexible Kari

system with better radar, more flexible software, smaller, faster computers, and "wireless" communications capability. Also, commercial satellite communications capability is also for sale with Russia selling GPS capability and satellite communications bandwidth to its former client states in addition to the illegal transfer of computer hardware mentioned earlier in this section.

The vulnerability for the US given the new Iraqi computer-based military environment is similar to that posed by the Iranians. The US goal is to gain information dominance over an adversary in conjunction in order to minimize the risks inherent in the use of more lethal forms of warfare. With access to the technologies examined in this section, the Iraqis could maintain their battlefield awareness and thus be better able to apply their numerical advantages in terms of armor and infantry forces at a time and place of their choosing. The result could be greater casualties by US forces responding to Iraqi aggression as opposed to the lightening ground victory seen in Operation Desert Storm.

Thus, economically, the conditions for an Iraqi rebuilding campaign are not far fetched and, apparently, not that far off. Also, coalition partners are having a much more difficult time selling the idea of punishing civilians for the sins of Saddam. Allowing the sale of oil to buy food and medicine is the first shot in a war by Saddam to rebuild his infrastructure. A coalition planner facing Desert Storm II could easily find a harder system to isolate and/or incapacitate.

> *Jan 2003...Task Force Entebbe, a force of Army helicopters lifted off from Al Jouf in western Saudi Arabia. Their objective—a night raid on two clusters of Soviet-made early warning radar just north of the Saudi-Iraqi border. The radars were van mounted and were the "eyes" of a surprisingly complex Iraqi networked air defense system known as Kari II. The initial salvo of missiles destroyed the radar vans presumably ensuring that the ensuing air attack of the selected Kari operations centers would*

have the element of surprise. An Iraqi special forces troop observed the raid from a nearby location and keyed commands into his personal communicator. His satellite comm link relayed details of the raid confirming what the Iraqi Colonel already knew from information automatically rerouted through his communications and computer network. "This battle will be different..." He watched as his forces moved to confront the raiders.

Notes

[1]*The General's War,* 106.

[2]*The General's War,* 106.

[3]*The Economist,* "France Starts to Open the Doors:Iraq and Sanctions," 14 January 1995

Chapter 8

Solutions

The United States has entered an era in which information is the dominate factor in competition between states in both the economic and military arena. From a military standpoint, the low cost of obtaining information age technologies will help potential adversaries of the US improve their military capabilities as they rapidly learn to leverage these technologies effectively [1]. US economic institutions are also vulnerable to information attack from more computer savvy state and non-state actors. Thus, action is necessary to gain and maintain information superiority. Inaction will doom the US militarily as her third world adversaries have recognized the information explosion and are in a race to exploit the advantages that technology provides.

A novice in the information warfare field may incorrectly assume that improved technology is the sole solution to overcoming enemy technological improvements. History tells us that this is not necessarily true. The US had a huge information technology advantage in Vietnam, only to be frustrated in its attempts to exploit that advantage. The Vietcong, while outgunned and technology poor, made use of a low tech information network at the tactical level allowing them to hit the enemy at time and place of their choosing unencumbered by the bureaucracy that shackled US command and control. The lesson hopefully learned from that conflict is that the way the technology is

organized and **implemented** is even more important than the technological superiority alone.

US third world adversaries continue to improve themselves with computer technology. As stated earlier, export controls are not the answer to availability as countries will simply buy from willing competitor nations. Also, as highlighted earlier, multinational corporations in the US and elsewhere are rapidly gaining approval to sell increasingly powerful computer hardware and software to third world countries and, given the rise of global economic trade agreements, this trend is expected to continue. Other answers are necessary.

One excellent approach is given by the Joint Staff in its 1997 pamphlet **Information Warfare: A Strategy for Peace...The Decisive Edge in War.** Three main points are discussed:

1. Educate and train US warriors in IW principles.
2. Pursue emerging technology that improves IW attack and defend capabilities
3. Build an organizational structure and relationship within the government and the nation that preserves the US information needs

In terms of education and training, the US should adopt a "spread the word" mentality at all levels of government that heightens the awareness of military and civilian agencies of the vulnerabilities inherent in computer systems and the steps that must be taken to reduce that risk. The Joint Staff leads the military implementation of policy and doctrine and the services should follow with their respective implementations. Awareness alone is not the answer, however. The US military must train, organize, and equip a cadre of information warriors in each service whose mission is to use computer technology to defend against computer attack and also to plot ways to cripple enemy computers.

The second factor is to pursue emerging technology. This is crucial to overcoming the continuing threat of increased availability of computer systems. The US must maintain gain and maintain the lead in computer technology by utilizing superior processes for identifying requirements, evaluating new technology, and acquiring that technology. This must be a constant process as computer technology will continue to improve.

However, the lessons of Vietnam must not be lost on US information warriors. The implementation of that technology combined with the appropriate organization and use is a must in order to defeat the probable adversaries in the 21st century. Organizationally, the US must recognize the type of foe likely to be encountered and organize its military and civilian agencies to combat that foe.

A good definition of likely foes is given by the RAND Corporation's John Arquilla and David Ronfeldt in their paper *Cyberwar is Coming*! They foresee more low intensity conflicts against the likes of international terrorists, guerrilla insurgents, drug cartels, and ethnic factions. Andrew Krepinvevich, a former Pentagon planner, foresees traditional foes such as Iran resorting to "street fighter" tactics.

In terms of technology, these foes will utilize cyberwarriors to attack American computer systems in an effort to deter the ability of the US to use its high technology advantages to secure a quick military victory as seen in Operation Desert Storm.

New technologies need to be pursued to address this threat.. The number one area for technology research and implementation in the military and civilian sector is the area of computer security. New computer security products that can isolate and disarm the increasing software attacks by cyberpunks and hackers are needed. Also, products that can rapidly track the attacker are needed in order to capture or deter future attacks.

These products should also have the ability to actively search for trojan horse programs that lay dormant and activate at a later time or place causing shutdowns or malfunctions. Other technologies that will address the threat posed by electronic terrorists include smaller, electromagnetic pulse resistant processors, personal recognition products, and jam-resistant communications. These technologies will defend against the loss of computer systems due to the detonation of a nuclear device, electronic intruders, and new products designed to monitor or disrupt communications. These technologies should be pursued as a defense against both the organized, financed hacker threat and the traditional state threat that the US will be up against in the future.

Another threat seen by experts is that US institutions, as currently organized, are vulnerable by the new breed of unorthodox groups organized as networks. These networks will be smaller and more difficult to detect due to their small size, their tremendous mobility, and their use of encrypted computer to computer communications. These networks are also dangerous due to their limited objective which is to inflict terror and havoc upon the US civilian and/or military community. A related vulnerability is that these groups are now better financed due to sponsorship by third world states. These groups will span state boundaries and increasingly use computers and encrypted computer networks to avoid signals intelligence. Their targets will be US commercial facilities such as banks, public transportation, and public telecommunications facilities.

The RAND Corporation believes that the US needs a different type of organization to combat this threat. They recommend technically proficient interagency teams consisting of military, intelligence community, Justice Department, State Department., Industry, and law enforcement to detect and defend against these groups. The goal

should not be additional bureaucracy but rather to provide leadership and direction to the multiple organizations seeking to involved in information warfare today. A lead agency concept will better focus efforts to protect American resources against attack improving upon the multiple efforts currently underway.

A domestic team, with the FBI as lead agency, should concentrate on detecting groups or individuals operating in the US and rapidly disseminating information on capabilities and intentions to their respective organizations for action. A combination of intelligence, detection, threat mitigation, and response can be achieved only through an interagency task force. Placing the FBI in charge will provide the leadership currently lacking in the war against terrorism.

Overseas or regional teams, led by the regional Commander in Chief (CINC), and consisting of the military, State Department., and intelligence community should be organized with emphasis on monitoring the technical capabilities and intentions of adversaries in their area of responsibility. This team should gather details on not only on an Iranian relationship with a client or client group, but also their technological capabilities, examining them for vulnerabilities that could be exploited at an appropriate time and place. Civilian agencies such as the FBI, for example, should augment military organizations planning the defense of the US against electronic attack. FBI liaisons at ACOM, for example, should assist in planning joint civilian-military training aimed at coordinating action against these attacks. The military is uniquely qualified for the training, coordination, and execution actions that these teams must employ to be successful.

The goal is to maintain the technological and information edge at all times and to be able to exploit that edge at a time and in a method of our choosing. The response may not be military. Information gathered by the unit may be used by the US civilian leadership to politically isolate the rouge state by exposing its relationship to a known terrorist. Economic sanctions and political pressure against the offending state would likely follow. The "launched" terrorist could also be identified, tracked, and destroyed by the interagency network in the same way an enemy missile would be based upon the information gathered. The key is to prevent the computer attack by gathering focused intelligence and responding with the appropriate force rather than the current policy of responding after the fact.

The critical lesson is that timely information is crucial so that the National Command Authority can make the appropriate decision on which instrument of power to use and how to use it to protect the security interests of the United States.

Notes

[1]David S.Alberts, *The Unintended Consequences of Information Age Technologies,* (Washington D.C., Library of Congress, 1996),10

Chapter 9

Conclusion

This research began by proposing four areas of concern:

1. Increase in availability of computer technology
2. Improvement in computer system capabilities in selected third world countries
3. Security ramifications of the proliferation in computer technology
4. Potential solutions for protection of US security interests

The first concern is computer proliferation to third world countries. A wide range of third world states and actors have been studied here in order to prove that computer technology is being rapidly proliferated providing the US with a rapidly changing strategic environment. As proven earlier, computer systems are more available to third world countries than ever before. However, history has shown that it is impossible to "put the genie back in the bottle" from a technology standpoint as has been the case with the spread of nuclear technology. Also, the new global economy has increased the spread of computer systems to the third world helping those countries to modernize their economies. Therefore, export restrictions alone will not guarantee security.

The second related concern is that third world countries are now in a position to use the available computer systems in a way which can possibly threaten US security. The US will no longer be able to count upon gaining information superiority on the battlefield unless new strategies are developed and implemented. This technology has become too inexpensive, too compact, and too redundant for military action to neutralize all of it[1].

One proposed solution is to constantly seek and maintain a technical superiority in certain critical computer technologies. Computer security products that defend against information attack must be acquired and constantly revalidated against a rapidly changing threat. Other technologies have been mentioned that defend against, track, and defeat computer attack must be constantly validated and acquired by the US in order to maintain the technological edge.

A second solution is to reorganize government agencies to combat the new electronic terrorists that pose a grave threat to US national security. New interagency teams organized domestically and overseas to detect and defeat the new network of foes to US interests are needed in this new strategic environment. Lead agencies should be assigned to the FBI domestically and the regional Commanders In Chief (CINC) for overseas threats. These lead agencies have a history of defending against threats to national security and can be adapted through training, education, and reorganization to lead the battle against computer technology threats. The regional CINC structure is unique to the US giving the country an advantage in its approach to conducting information operations. Other countries, friend and foe, without the global emphasis and reach of the US will be at a disadvantage in their approach to dealing with global computer attack.

Education and training must also be a constant in the US strategy to maintain information superiority over its foes. Military units, for example, should be trained specifically to exploit enemy vulnerabilities resulting from the new third world computer environment.

Another solution offered was to use the new interagency team to gather focused intelligence, disseminate warnings and indications to the appropriate agencies, and respond with the appropriate force against computer attacks.

Finally, the US must be smarter in the implementation of new technology than its adversaries, educate civilian and military personnel from top to bottom on IW threats and policies, and, finally, provide authorities with intelligence, intelligence, and more intelligence on the new threats to US national security.

Notes

[1]Winn Swartau, *Information Warfare,* 2nd ed. (New York: Thunder's Mouth Press, 1996), p446.

Bibliography

Alberts, David S., *The Unintended Consequences of Information Age Technologies,* National Defense University, 1996.

Cloud, David S., "Critics Fear GATT May Declare Open Season on US Laws," Congressional Quarterly, 23 July 1994.

Chairman of the Joint Chiefs of Staff, *Information Warfare: A Strategy for Peace...The Decisive Edge in War,* Washington DC: Government Printing Office, September 1996.

Dedrick, Jason and Kraemer, Kenneth, *Asian Survey,* May 1993.

The Economist, "France Starts to Open the Doors: Iraq and Sanctions, 14 January 1995.

Electronic News, 16 January 1995.

Bearman, Jonathan, *The Oil Daily, 13* August 1996.

Michael Gordon and Bernard Trainor, *The General's War: The Inside Story of the Conflict in the Gulf,* Little, Brown, and Company, 1995.

Jayaraman, K.S., *Nature,* "Pakistani Virus Invades Indian Neighbor," 13 April 1989.

Kapitza, Sergei, *The Bulletin of the Atomic Scientists,* May 1992.

The Oil Daily, "US Decides Against Sanctions Over Sales of Nuclear Technology to Pakistan," 13 May 1996.

Perryman, M., "US Industry Remains Dominant Player in Global Markets," *San Antonio Business Journal,* 21 June 1996

Schroeder Michael and Armstrong, Larry, "The Push to Plug Iran's Technology Pipeline," *Business Week,* 14 June 1993.

Swartau, Winn, *Information Warfare,* 2nd ed., New York: Thunder's Mouth Press, 1996.

Stremlau, John, *Foreign Policy,* "Dateline Bangalore: Third World Technopolis," Spring 1996.

Thompson, Mark, *Time Magazine* ,"If War Comes Home," 21 August 1996.

Time Magazine, "The Pyongyang-Jerusalem Connection," 31 May 1993.

Vahid, Saeed, *Byte,* "Moving Forward Cautiously," October 1993.

Waller, Douglas, *Time Magazine,* "Onward Cyber Soldiers, 21 August 1996.

Zachary G., *The Wall Street Journal,* "U.S. Software: Now It May Be Made in Bulgaria," 21 February 1995.

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air Command and Staff College
Maxwell AFB, Al 36112